

<i>SERFF Tracking Number:</i>	<i>CNNA-125314121</i>	<i>State:</i>	<i>Arkansas</i>
<i>Filing Company:</i>	<i>The Cincinnati Insurance Company</i>	<i>State Tracking Number:</i>	<i>AR-PC-07-026341</i>
<i>Company Tracking Number:</i>	<i>CBD-07-6023-AR</i>		
<i>TOI:</i>	<i>23.0 Fidelity</i>	<i>Sub-TOI:</i>	<i>23.0000 Fidelity</i>
<i>Product Name:</i>	<i>CBD-07-6023-AR</i>		
<i>Project Name/Number:</i>	<i>/</i>		

Filing at a Glance

Company: The Cincinnati Insurance Company

Product Name: CBD-07-6023-AR

TOI: 23.0 Fidelity

Sub-TOI: 23.0000 Fidelity

Filing Type: Form

SERFF Tr Num: CNNA-125314121 State: Arkansas

SERFF Status: Closed

Co Tr Num: CBD-07-6023-AR

Co Status:

Author: Sharon Grubbs

Date Submitted: 10/05/2007

State Tr Num: AR-PC-07-026341

State Status:

Reviewer(s): Betty Montesi,
Llyweyia Rawlins, Brittany Yielding

Disposition Date: 10/09/2007

Disposition Status: Approved

Effective Date (New): 05/01/2008

Effective Date (Renewal):

Effective Date Requested (New): 05/01/2008

Effective Date Requested (Renewal):

General Information

Project Name:

Project Number:

Reference Organization:

Reference Title:

Filing Status Changed: 10/09/2007

State Status Changed: 10/05/2007

Corresponding Filing Tracking Number:

Filing Description:

At this time, we wish to file form(s) per the attached memorandum.

Status of Filing in Domicile: Pending

Domicile Status Comments:

Reference Number:

Advisory Org. Circular:

Deemer Date:

Final copies are attached for your review.

Filing fees will be sent through the Electronic Filing Fee System as a (EFT) filing.

Please be advised that we work on a 90-days-in-advance schedule. As a result, we would appreciate your approval by February 1, 2008, for the software to be mailed to our agents on March 1, 2008, for the effective date of May 1, 2008.

Your approval is respectfully requested for use on policies effective on or after May 1, 2008.

SERFF Tracking Number:	CNNA-125314121	State:	Arkansas
Filing Company:	The Cincinnati Insurance Company	State Tracking Number:	AR-PC-07-026341
Company Tracking Number:	CBD-07-6023-AR		
TOI:	23.0 Fidelity	Sub-TOI:	23.0000 Fidelity
Product Name:	CBD-07-6023-AR		
Project Name/Number:	/		

Company and Contact

Filing Contact Information

Sharon Grubbs, Senior Filings Analyst
6200 S. Gilmore Road
Fairfield, OH 45014

sharon_grubbs@cinfin.com
(513) 870-2091 [Phone]
()-[FAX]

Filing Company Information

The Cincinnati Insurance Company
6200 S. Gilmore Road
Fairfield, OH 45014
(513) 870-2000 ext. [Phone]

CoCode: 10677
Group Code: 244
Group Name:
FEIN Number: 31-0542366

State of Domicile: Ohio
Company Type:
State ID Number:

Filing Fees

Fee Required?	Yes
Fee Amount:	\$50.00
Retaliatory?	Yes
Fee Explanation:	
Per Company:	No

COMPANY	AMOUNT	DATE PROCESSED	TRANSACTION #
The Cincinnati Insurance Company	\$50.00	10/05/2007	15969225

SERFF Tracking Number:	CNNA-125314121	State:	Arkansas
Filing Company:	The Cincinnati Insurance Company	State Tracking Number:	AR-PC-07-026341
Company Tracking Number:	CBD-07-6023-AR		
TOI:	23.0 Fidelity	Sub-TOI:	23.0000 Fidelity
Product Name:	CBD-07-6023-AR		
Project Name/Number:	/		

Correspondence Summary

Dispositions

Status	Created By	Created On	Date Submitted
Approved	Llyweyia Rawlins	10/09/2007	10/09/2007

SERFF Tracking Number: *CNNA-125314121*

State: *Arkansas*

Filing Company: *The Cincinnati Insurance Company*

State Tracking Number: *AR-PC-07-026341*

Company Tracking Number: *CBD-07-6023-AR*

TOI: *23.0 Fidelity*

Sub-TOI: *23.0000 Fidelity*

Product Name: *CBD-07-6023-AR*

Project Name/Number: */*

Disposition

Disposition Date: 10/09/2007

Effective Date (New): 05/01/2008

Effective Date (Renewal):

Status: Approved

Comment:

Rate data does NOT apply to filing.

SERFF Tracking Number: CNNA-125314121 State: Arkansas

Filing Company: The Cincinnati Insurance Company State Tracking Number: AR-PC-07-026341

Company Tracking Number: CBD-07-6023-AR

TOI: 23.0 Fidelity Sub-TOI: 23.0000 Fidelity

Product Name: CBD-07-6023-AR

Project Name/Number: /

Item Type	Item Name	Item Status	Public Access
Supporting Document	Uniform Transmittal Document-Property & Casualty	Approved	Yes
Supporting Document	PROPRETY AND CASUALTY TRANSMITTAL	Approved	Yes
Supporting Document	FORM FILING SCHEDULE	Approved	Yes
Supporting Document	MEMORANDUM	Approved	Yes
Form	PROPOSAL FOR CINCINNATI'S "BLUE CHIP" INSURANCE PROGRAM FOR FINANCIAL INSTITUTIONS - INTERNET AND ELECTRONIC BANKING COVERAGE PART VI	Approved	Yes
Form	RENEWAL PROPOSAL FOR CINCINNATI'S "BLUE CHIP" INSURANCE PROGRAM FOR FINANCIAL INSTITUTIONS - INTERNET AND ELECTRONIC BANKING COVERAGE PART VI	Approved	Yes

SERFF Tracking Number: CNNA-125314121 State: Arkansas
 Filing Company: The Cincinnati Insurance Company State Tracking Number: AR-PC-07-026341
 Company Tracking Number: CBD-07-6023-AR
 TOI: 23.0 Fidelity Sub-TOI: 23.0000 Fidelity
 Product Name: CBD-07-6023-AR
 Project Name/Number: /

Form Schedule

Review Status	Form Name	Form #	Edition Date	Form Type Action	Action Specific Data	Readability	Attachment
Approved	PROPOSAL FOR BC 010 CINCINNATI'S "BLUE CHIP" INSURANCE PROGRAM FOR FINANCIAL INSTITUTIONS - INTERNET AND ELECTRONIC BANKING COVERAGE PART VI		11 07	Application/ Replaced Binder/Enro llment	Replaced Form #:0.00 BC 010 10 07 Previous Filing #: CBD-07-6020-AR		BC010 11-07.pdf
Approved	RENEWAL PROPOSAL FOR CINCINNATI'S "BLUE CHIP" INSURANCE PROGRAM FOR FINANCIAL INSTITUTIONS - INTERNET AND ELECTRONIC BANKING COVERAGE PART VI	BC 011	11 07	Application/ Replaced Binder/Enro llment	Replaced Form #:0.00 BC 011 10 07 Previous Filing #: CBD-07-6020-AR		BC011 11-07.pdf

**THE CINCINNATI INSURANCE COMPANY
PROPOSAL FOR
CINCINNATI'S "BLUE CHIP" INSURANCE PROGRAM
FOR FINANCIAL INSTITUTIONS**

INTERNET AND ELECTRONIC BANKING COVERAGE (PART VI)

GENERAL INFORMATION

1. Name of company and names of all owned subsidiaries: _____

2. Mailing Address: _____
3. List all website URL's and static IP addresses utilized by the company and its subsidiaries:

4. Identify the consumer or commercial services that will be available within the year at the addresses listed in number 3 above:
- | | | | |
|--|--|---|---------------------------------------|
| <input type="checkbox"/> Account Management | <input type="checkbox"/> Trust Services | <input type="checkbox"/> Brokerage Advisory | <input type="checkbox"/> Bill Payment |
| <input type="checkbox"/> Investment Banking | <input type="checkbox"/> Insurance Agency | <input type="checkbox"/> Submission of Loan / Credit Card Application | |
| <input type="checkbox"/> None (Web content only) | <input type="checkbox"/> Change of Address | <input type="checkbox"/> Funds Transfer | <input type="checkbox"/> Other: _____ |
5. Names, titles and phone numbers of individuals assigned by the board to be responsible for implementation of the information security program:

6. Name, title, phone number and e-mail address of the individual or vendor responsible for website security:
- ☐ Individual from number 5 above: _____
- ☐ Vendor contact information: _____
7. List any non-banking professional services provided by the company:

Sections I - V should be completed by the Information Security Officer

I. INFORMATION SECURITY AND COMPLIANCE PROGRAMS

8. List the qualifications of the individuals in number 5 above relevant to information security:
- | | |
|--|----------------|
| <input type="checkbox"/> Education | Explain: _____ |
| <input type="checkbox"/> Certification | Explain: _____ |
| <input type="checkbox"/> Experience | Explain: _____ |
9. What methods do security staff use to stay informed of information security issues that effect the industry, including but not limited to security incidents, new security threats / risks / vulnerabilities, malware outbreaks, new security technologies, new laws and security standards:

- ☐ Management involvement in CISO roundtables
- ☐ Involvement in information security organizations or associations
- ☐ Receipt of automated vulnerability / threat alerts from non-profit security organizations or associations
- ☐ Daily review of information security websites
- ☐ Receipt of customized security alerts from security vendor
- ☐ Receipt of automated security announcements from current vendors
- ☐ Other: _____

10. Do those who can access customer data, including employees, board members, on site vendors and independent contractors, receive annual information security and privacy training that includes: ☐ Yes ☐ No
- how to identify and report information security vulnerabilities and incidents
 - classification and appropriate use of information
 - appropriate use of Internet, e-mail, IM, file downloads, personally owned devices, wireless
11. Does the company have written information security policies or procedures that address: ☐ Yes ☐ No
- a.) Confidentiality, availability and integrity of information as required by regulations, statutes and standards that are applicable to the company, which may include CAN-SPAM, COPPA, FCRA, FTC guidance, HIPAA, PCI, security breach notification laws, SOX and international law? ☐ Yes ☐ No
 - b.) Gramm-Leach-Bliley Act per 16 C.F.R. Part 314 ☐ Yes ☐ No
 - c.) Employee sanctions for security policy violations? ☐ Yes ☐ No
 - d.) Development and implementation of secure information systems including software and hardware? ☐ Yes ☐ No
12. Name and e-mail address of the individual in number 5 above responsible for receiving and coordinating responses to significant information security incidents and formally responding to information security audit findings:
- _____
13. Has a qualified attorney reviewed: ☐ Yes ☐ No
- a.) The Company privacy policy and website privacy policy? ☐ Yes ☐ No
 - b.) The legal requirements of the applicable regulations, statutes and standards from number 11? ☐ Yes ☐ No
 - c.) Website content for intellectual property violations or other intellectual property issues, including searchable content, domain names, and third party content linked to or in frames? ☐ Yes ☐ No
14. Are security recommendations from hardware and software vendors implemented, including installation of critical security patches? ☐ Yes ☐ No
15. Describe here, or on an attachment, any compensating security controls for questions answered "no" in Section I:
- _____
- _____

II. INTERNET AND ELECTRONIC BANKING

16. What percentage of consumer and commercial customers use the company website?
- ☐ 1 - 25% ☐ 26 - 50% ☐ 51 - 75% ☐ 75 - 100%
17. Does the company post a compliant privacy policy on its website that accurately describes its privacy practices? ☐ Yes ☐ No
18. Are customer electronic transactions and funds transfers, both interactive and batch, protected from unauthorized modifications by reasonable and appropriate use of the following: encrypted transmission and storage, verification of questionable activity or failed access, multi-factor authentication for customers, non-repudiation controls, two-factor authentication of support personnel, and database integrity controls? ☐ Yes ☐ No
19. Are customers using the website advised how to protect their accounts, non-public information, or financial transactions? ☐ Yes ☐ No
20. Does the company have technical and procedural controls to protect customers from phishing, pharming and similar attacks? ☐ Yes ☐ No
21. Identify any services provided by vendors to support the company Internet banking site such as website development / hosting, security, monitoring, incident response, backend processing. List any software packages purchased for core processing or Internet banking services.

Vendor name and associated services / software: _____

22. How many times in the last five years has the company, its website or other computer system been a specific target of an electronic attack such as phishing, pharming, website vandalism, denial of service or keylogger?

☐ None ☐ Once ☐ Two or more

If once or more, describe the event on an attachment, including the timeframe for detection, the impact to customers and the controls established to prevent subsequent events.

23. Are procedures and / or technologies in place to assure the availability of customer website services and funds transfer services during hardware / software failures, physical disasters, system performance degradations, denial of service attacks, or disruptions of power or communications services? ☐ Yes ☐ No

24. Which certifications, if any, does the information security program, privacy program or website currently hold?

Attach proof of certification.

☐ VeriSign ☐ eTrust ☐ CyberTrust ☐ ISO270001
☐ TRUSTe ☐ PCI ☐ Other: _____

25. Does the company have a network firewall that is properly maintained to:

a.) Separate company hardware accessible from the Internet from hardware that stores customer data?

☐ Yes ☐ No

b.) Separate hardware that stores customer data from any non-production systems?

☐ Yes ☐ No

c.) Deny use of ports that are not currently authorized for use?

☐ Yes ☐ No

d.) Protect workstations from Internet threats?

☐ Yes ☐ No

26. If employees, customers, vendors or other individuals remotely access systems that are in an internal network segment, are they required to use two-factor authentication, encrypted transmissions and a workstation firewall? ☐ Yes ☐ No

27. Describe here, or on an attachment, any compensating security controls for questions answered "no" in Section II:

III. ACCESS TO SYSTEMS AND DATA

28. Is each individual employee, board member, customer, vendor and independent contractor required to have a unique login account to access computing systems that may contain customer data? ☐ Yes ☐ No

a.) Does each account have an associated personal identification number (PIN) or unique password? ☐ Yes ☐ No

b.) Are all passwords encrypted when electronically stored and transmitted? ☐ Yes ☐ No

c.) Are individuals provided procedures describing how to protect accounts and passwords? ☐ Yes ☐ No

29. Are individuals, including employees, board members, IT support personnel, customers, vendors and independent contractors, granted access to confidential and transactional information only as required, and is access revoked when no longer required? ☐ Yes ☐ No

30. If service providers or other third parties have on-site, off-site or remote access to electronic customer data, are they required by written agreement to implement security controls designed to meet the objectives of the company's information security program, including training, access controls, monitoring, third party audits, and notifying the company of security incidents involving customer data? ☐ Yes ☐ No

31. Do you require vendors to maintain insurance for misconduct, errors, omissions and negligence? ☐ Yes ☐ No

32. Are reasonable and appropriate controls in place to protect login accounts, which may include, but are not limited to password expirations, account lockout for attempted use of incorrect password, minimum password length, inactive account time-out, disablement of unused accounts, multifactor authentication, and policies against sharing accounts / passwords? ☐ Yes ☐ No

33. Are computing systems designed, developed and configured to restrict access to only authorized users and support personnel? ☐ Yes ☐ No

34. Are formal procedures in place to control changes to production systems, including software and hardware? ☐ Yes ☐ No

35. Is customer information that is stored on mobile devices or electronic media encrypted when it is off site? ☐ Yes ☐ No

36. Describe here, or on an attachment, any compensating security controls for questions answered "no" in Section III:

IV. MONITORING AND INCIDENT RESPONSE

37. Are procedures in place to generate, regularly analyze, respond to and preserve the following security logs to detect unauthorized activity: network access, website access, customer Internet banking database access, restricted transactions, corrected / revised financial transactions, firewall, intrusion detection / prevention, anti-virus, anti-spyware and anti-fraud systems? ☐ Yes ☐ No

38. In the last two years, has the company sustained unscheduled system downtime, a denial of service, a successful intrusion attempt, electronic fraud, unauthorized disclosure, theft or loss of data, tampering, or unauthorized installation of a keylogger, rootkit, or backdoor program? ☐ Yes ☐ No

If yes, describe the event on an attachment, including the timeframe for detection, the impact to customers and the controls established to prevent subsequent events.

39. Is the time on all systems synchronized to facilitate analysis of logs? ☐ Yes ☐ No

40. Does the company have an intrusion detection or prevention system that protects critical systems, including but not limited to Internet banking and related systems? ☐ Yes ☐ No

41. Is anti-virus software properly installed and maintained on personal computers, critical servers and other hardware that is directly connected to the company network, including hardware of affiliates, vendors and business partners? ☐ Yes ☐ No

42. Does each system display a banner notifying users that activity is monitored and that the system is restricted to authorized use only? ☐ Yes ☐ No

43. How is the integrity of security logs preserved for potential use in legal proceedings?

- ☐ Following formal incident response procedures (**Attach a copy.**)
☐ Oversight by forensic specialist - Name / title or vendor name: _____
☐ Other: _____
☐ Not addressed at this time

44. Is an appropriately trained IT security team available 24x7 to respond to viruses, unauthorized access and other security incidents? ☐ Yes ☐ No

45. Describe here, or on an attachment, any compensating security controls for questions answered "no" in Section IV:

V. AUDITS AND REVIEW

46. Are annual audits of physical, procedural and technical security controls performed by an independent security auditing organization with a CISSP or CISA certified practitioner on staff? ☐ Yes ☐ No
If "yes", name the vendor security organization(s):

47. Are vulnerability tests conducted at least annually on the following to make sure they perform as expected:

- | | | |
|--|------------------------------|-----------------------------|
| a.) External firewall? | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| b.) Intrusion detection / prevention systems? | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| c.) Website authentication services? | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| d.) Website software? | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| e.) Website servers and customer database servers? | <input type="checkbox"/> Yes | <input type="checkbox"/> No |

48. Have all significant security risks identified by audit deficiencies, regulatory criticisms, vulnerability tests or exploited vulnerabilities been remediated? ☐ Yes ☐ No

If "no", indicate outstanding items and status of remediation on an attachment.

49. Is the individual in number 12 responsible for reporting the status of the program to executive management and / or the board of directors and if so, what is the frequency?

☐ No ☐ Longer than annually ☐ Annually ☐ Quarterly ☐ Monthly

50. At what frequency are information security and privacy policies reviewed and updated to reflect changes in business process, use of technology, new technology or software, security best-practices, and the regulatory environment?

☐ Monthly ☐ Quarterly ☐ Annually ☐ Longer than Annually

51. Does the information security program use a formal scoring or prioritization process for managing information security risks? ☐ Yes ☐ No

52. Within the last 12 months has the computer obtained an updated SAS70 Type II or other security audit for each vendor with access to electronic customer information? ☐ Yes ☐ No
☐ No vendors with access

53. Is the individual in number 12 responsible for monitoring the effectiveness of security procedures and controls? ☐ Yes ☐ No

54. Describe here, or on an attachment, any compensating security controls for questions answered "no" in Section V:

VI. INSURANCE COVERAGES AND UNDERWRITING INFORMATION

1. Do you currently have the prior or current insurance coverage listed below?

Coverage Type	Yes	No	Insurer	Limits	Deductible	Policy Period
Employment Liability						
Fiduciary Liability						
D&O Liability						
Trust Errors and Omissions Liability						
Internet and Electronic Banking Liability for FI						
Bankers Professional Liability						
Bankers Blanket Bond						

2. Coverage Requested

Coverage Type	Desired Limit	Desired Deductible
Internet and Electronic Banking Coverage		

3. Additional Underwriting Materials Requested

As part of this application, please attach the following:

- Attach proof of certification, if applicable (question number 24)
- Attach a description of previous security events (question numbers 22 and 38)
- Attach a description of outstanding risks and status of remediation efforts (question number 48)
- Attach a description of compensating controls (question numbers 15, 27, 38, 45 and 54)

4. Additional Underwriting Materials that may be Requested

As part of this application review process, CIC may request the following:

- Attach a representative sample of the information security provisions of third party vendor contracts (question number 30)
- Attach photocopy of website privacy policy and security statements (question number 17)
- Attach a photocopy of executive summary of the recent independent security audit for each vendor (question number 52)
- Attach a photocopy of security incident response procedures (question number 43)
- Attach a photocopy of the executive summary of the most recent independent IT security audit (question number 46)

VII. PRIOR KNOWLEDGE / WARRANTY DECLARATIONS

1. No claim which, if insurance had been in force similar to that now applied for, which would have fallen within the scope of such insurance, has been made or is now pending against any person proposed for insurance in the capacity of either Director, Officer or employee of the above-stated Company, except as follows (if answer is none, so indicate):

2. No person proposed for this insurance is cognizant of any act, error, or omission which he has reason to suppose might afford valid grounds for any future claim such as would fall within the scope of the proposed insurance, except as follows (if answer is none, so state):

3. The Company and / or its Directors and Officers and employees have not been involved in or have any knowledge of any anti-trust, tax, or copyright litigation or government regulatory or administrative proceedings, except as follows (if answer is none, so indicate):

4. No fact, circumstance or situation indicating the probability of a claim or action against which indemnification would be afforded by the proposed insurance is now known by any person(s) or entity(ies) proposed for this insurance other than that which is disclosed in this Proposal. It is agreed by all concerned that if there be knowledge of any such fact, circumstance, or situation, any claim subsequently emanating therefrom shall be excluded from coverage under the proposed insurance.

The undersigned authorized agent of the person(s) and entity(ies) proposed for this insurance for the purpose of this Proposal warrants that to the best of his knowledge the statements herein are true; and it is agreed that this Proposal shall be the basis of the contract and be deemed incorporated therein should the insurer evidence its acceptance of this Proposal by issuance of a policy. This Proposal will be attached to and will become part of such policy, if issued.

Attached and made a part of this Proposal by reference is one copy of each of the following: the Company's most recent Annual Report and Statement of Condition to Stockholders, certified provisions of the Charter or Bylaws covering Indemnification of Directors and Officers, and Notice to Stockholders and Proxy Statement for either the last or the next annual meeting.

The Cincinnati Insurance Company is hereby authorized to make any investigation, inquiry and on-site security review in connection with this Proposal as it deems necessary.

The undersigned authorizes the release of claim information from any prior insurer to The Cincinnati Insurance Company.

Signing this Proposal does not bind the Company or The Cincinnati Insurance Company to complete the insurance.

PLEASE REVIEW CAREFULLY. Except to such extent as may be otherwise in the policy, the policy for which this Proposal is being made is limited for ONLY CLAIMS THAT ARE FIRST MADE AGAINST THE INSURED WHILE THE POLICY IS IN FORCE.

NOTICE TO OHIO APPLICANTS: ANY PERSON WHO, WITH INTENT TO DEFRAUD OR KNOWING THAT HE / SHE IS FACILITATING A FRAUD AGAINST AN INSURER, SUBMITS AN APPLICATION OR FILES A CLAIM CONTAINING A FALSE OR DECEPTIVE STATEMENT IS GUILTY OF INSURANCE FRAUD.

WARNING: ANY PERSON WHO KNOWINGLY AND WITH INTENT TO DEFRAUD ANY INSURANCE COMPANY OR ANOTHER PERSON FILES AN APPLICATION FOR INSURANCE OR STATEMENT OF CLAIM CONTAINING ANY MATERIALLY FALSE INFORMATION, OR CONCEALS FOR THE PURPOSE OF MISLEADING INFORMATION CONCERNING ANY FACT MATERIAL THERETO, COMMITS A FRAUDULENT INSURANCE ACT, WHICH IS A CRIME AND SUBJECTS (VT: MAY BE COMMITTING A CRIME SUBJECTING) THE PERSON TO CRIMINAL AND (NY: SUBSTANTIAL) CIVIL PENALTIES. IN THE DISTRICT OF COLUMBIA, LOUISIANA, MAINE, TENNESSEE, VIRGINIA AND WASHINGTON, INSURANCE BENEFITS MAY ALSO BE DENIED.

Signed: _____
Chairman of the Board, President or comparable officer

Printed Name: _____

Title: _____

Date: _____

Signed: _____
Information Security Officer or comparable officer

Printed Name: _____

Title: _____

Date: _____

Agent's Signature **Date**

Agency and Code Number

**THE CINCINNATI INSURANCE COMPANY
RENEWAL PROPOSAL FOR
CINCINNATI'S "BLUE CHIP" INSURANCE PROGRAM
FOR FINANCIAL INSTITUTIONS**

INTERNET AND ELECTRONIC BANKING COVERAGE (PART VI)

GENERAL INFORMATION

1. Name of company and names of all owned subsidiaries: _____

2. Mailing Address: _____
3. List all website URL's and static IP addresses utilized by the company and its subsidiaries:

4. Identify the consumer or commercial services that will be available within the year at the addresses listed in number 3 above:
- | | | | |
|--|--|---|---------------------------------------|
| <input type="checkbox"/> Account Management | <input type="checkbox"/> Trust Services | <input type="checkbox"/> Brokerage Advisory | <input type="checkbox"/> Bill Payment |
| <input type="checkbox"/> Investment Banking | <input type="checkbox"/> Insurance Agency | <input type="checkbox"/> Submission of Loan / Credit Card Application | |
| <input type="checkbox"/> None (Web content only) | <input type="checkbox"/> Change of Address | <input type="checkbox"/> Funds Transfer | <input type="checkbox"/> Other: _____ |
5. Names, titles and phone numbers of individuals assigned by the board to be responsible for implementation of the information security program:

6. Name, title, phone number and e-mail address of the individual or vendor responsible for website security:
- ☐ Individual from number 5 above: _____
- ☐ Vendor contact information: _____
7. List any non-banking professional services provided by the company:

Sections I - V should be completed by the Information Security Officer

I. INFORMATION SECURITY AND COMPLIANCE PROGRAMS

8. List the qualifications of the individuals in number 5 above relevant to information security:
- | | |
|--|----------------|
| <input type="checkbox"/> Education | Explain: _____ |
| <input type="checkbox"/> Certification | Explain: _____ |
| <input type="checkbox"/> Experience | Explain: _____ |
9. What methods do security staff use to stay informed of information security issues that effect the industry, including but not limited to security incidents, new security threats / risks / vulnerabilities, malware outbreaks, new security technologies, new laws and security standards:

- ☐ Management involvement in CISO roundtables
- ☐ Involvement in information security organizations or associations
- ☐ Receipt of automated vulnerability / threat alerts from non-profit security organizations or associations
- ☐ Daily review of information security websites
- ☐ Receipt of customized security alerts from security vendor
- ☐ Receipt of automated security announcements from current vendors
- ☐ Other: _____

10. Do those who can access customer data, including employees, board members, on site vendors and independent contractors, receive annual information security and privacy training that includes: ☐ Yes ☐ No
- how to identify and report information security vulnerabilities and incidents
 - classification and appropriate use of information
 - appropriate use of Internet, e-mail, IM, file downloads, personally owned devices, wireless
11. Does the company have written information security policies or procedures that address: ☐ Yes ☐ No
- a.) Confidentiality, availability and integrity of information as required by regulations, statutes and standards that are applicable to the company, which may include CAN-SPAM, COPPA, FCRA, FTC guidance, HIPAA, PCI, security breach notification laws, SOX and international law? ☐ Yes ☐ No
 - b.) Gramm-Leach-Bliley Act per 16 C.F.R. Part 314 ☐ Yes ☐ No
 - c.) Employee sanctions for security policy violations? ☐ Yes ☐ No
 - d.) Development and implementation of secure information systems including software and hardware? ☐ Yes ☐ No
12. Name and e-mail address of the individual in number 5 above responsible for receiving and coordinating responses to significant information security incidents and formally responding to information security audit findings:
- _____
13. Has a qualified attorney reviewed: ☐ Yes ☐ No
- a.) The Company privacy policy and website privacy policy? ☐ Yes ☐ No
 - b.) The legal requirements of the applicable regulations, statutes and standards from number 11? ☐ Yes ☐ No
 - c.) Website content for intellectual property violations or other intellectual property issues, including searchable content, domain names, and third party content linked to or in frames? ☐ Yes ☐ No
14. Are security recommendations from hardware and software vendors implemented, including installation of critical security patches? ☐ Yes ☐ No
15. Describe here, or on an attachment, any compensating security controls for questions answered "no" in Section I:
- _____
- _____

II. INTERNET AND ELECTRONIC BANKING

16. What percentage of consumer and commercial customers use the company website?
- ☐ 1 - 25% ☐ 26 - 50% ☐ 51 - 75% ☐ 75 - 100%
17. Does the company post a compliant privacy policy on its website that accurately describes its privacy practices? ☐ Yes ☐ No
18. Are customer electronic transactions and funds transfers, both interactive and batch, protected from unauthorized modifications by reasonable and appropriate use of the following: encrypted transmission and storage, verification of questionable activity or failed access, multi-factor authentication for customers, non-repudiation controls, two-factor authentication of support personnel, and database integrity controls? ☐ Yes ☐ No
19. Are customers using the website advised how to protect their accounts, non-public information, or financial transactions? ☐ Yes ☐ No
20. Does the company have technical and procedural controls to protect customers from phishing, pharming and similar attacks? ☐ Yes ☐ No
21. Identify any services provided by vendors to support the company Internet banking site such as website development / hosting, security, monitoring, incident response, backend processing. List any software packages purchased for core processing or Internet banking services.

Vendor name and associated services / software: _____

22. How many times in the last five years has the company, its website or other computer system been a specific target of an electronic attack such as phishing, pharming, website vandalism, denial of service or keylogger?

☐ None ☐ Once ☐ Two or more

If once or more, describe the event on an attachment, including the timeframe for detection, the impact to customers and the controls established to prevent subsequent events.

23. Are procedures and / or technologies in place to assure the availability of customer website services and funds transfer services during hardware / software failures, physical disasters, system performance degradations, denial of service attacks, or disruptions of power or communications services? ☐ Yes ☐ No

24. Which certifications, if any, does the information security program, privacy program or website currently hold?

Attach proof of certification.

☐ VeriSign ☐ eTrust ☐ CyberTrust ☐ ISO270001
☐ TRUSTe ☐ PCI ☐ Other: _____

25. Does the company have a network firewall that is properly maintained to:

a.) Separate company hardware accessible from the Internet from hardware that stores customer data?

☐ Yes ☐ No

b.) Separate hardware that stores customer data from any non-production systems?

☐ Yes ☐ No

c.) Deny use of ports that are not currently authorized for use?

☐ Yes ☐ No

d.) Protect workstations from Internet threats?

☐ Yes ☐ No

26. If employees, customers, vendors or other individuals remotely access systems that are in an internal network segment, are they required to use two-factor authentication, encrypted transmissions and a workstation firewall? ☐ Yes ☐ No

27. Describe here, or on an attachment, any compensating security controls for questions answered "no" in Section II:

III. ACCESS TO SYSTEMS AND DATA

28. Is each individual employee, board member, customer, vendor and independent contractor required to have a unique login account to access computing systems that may contain customer data? ☐ Yes ☐ No

a.) Does each account have an associated personal identification number (PIN) or unique password? ☐ Yes ☐ No

b.) Are all passwords encrypted when electronically stored and transmitted? ☐ Yes ☐ No

c.) Are individuals provided procedures describing how to protect accounts and passwords? ☐ Yes ☐ No

29. Are individuals, including employees, board members, IT support personnel, customers, vendors and independent contractors, granted access to confidential and transactional information only as required, and is access revoked when no longer required? ☐ Yes ☐ No

30. If service providers or other third parties have on-site, off-site or remote access to electronic customer data, are they required by written agreement to implement security controls designed to meet the objectives of the company's information security program, including training, access controls, monitoring, third party audits, and notifying the company of security incidents involving customer data? ☐ Yes ☐ No

31. Do you require vendors to maintain insurance for misconduct, errors, omissions and negligence? ☐ Yes ☐ No

32. Are reasonable and appropriate controls in place to protect login accounts, which may include, but are not limited to password expirations, account lockout for attempted use of incorrect password, minimum password length, inactive account time-out, disablement of unused accounts, multifactor authentication, and policies against sharing accounts / passwords? ☐ Yes ☐ No

33. Are computing systems designed, developed and configured to restrict access to only authorized users and support personnel? ☐ Yes ☐ No

34. Are formal procedures in place to control changes to production systems, including software and hardware? ☐ Yes ☐ No

35. Is customer information that is stored on mobile devices or electronic media encrypted when it is off site? ☐ Yes ☐ No

36. Describe here, or on an attachment, any compensating security controls for questions answered "no" in Section III:

IV. MONITORING AND INCIDENT RESPONSE

37. Are procedures in place to generate, regularly analyze, respond to and preserve the following security logs to detect unauthorized activity: network access, website access, customer Internet banking database access, restricted transactions, corrected / revised financial transactions, firewall, intrusion detection / prevention, anti-virus, anti-spyware and anti-fraud systems? ☐ Yes ☐ No

38. In the last two years, has the company sustained unscheduled system downtime, a denial of service, a successful intrusion attempt, electronic fraud, unauthorized disclosure, theft or loss of data, tampering, or unauthorized installation of a keylogger, rootkit, or backdoor program? ☐ Yes ☐ No

If yes, describe the event on an attachment, including the timeframe for detection, the impact to customers and the controls established to prevent subsequent events.

39. Is the time on all systems synchronized to facilitate analysis of logs? ☐ Yes ☐ No

40. Does the company have an intrusion detection or prevention system that protects critical systems, including but not limited to Internet banking and related systems? ☐ Yes ☐ No

41. Is anti-virus software properly installed and maintained on personal computers, critical servers and other hardware that is directly connected to the company network, including hardware of affiliates, vendors and business partners? ☐ Yes ☐ No

42. Does each system display a banner notifying users that activity is monitored and that the system is restricted to authorized use only? ☐ Yes ☐ No

43. How is the integrity of security logs preserved for potential use in legal proceedings?

☐ Following formal incident response procedures (**Attach a copy.**)

☐ Oversight by forensic specialist - Name / title or vendor name: _____

☐ Other: _____

☐ Not addressed at this time

44. Is an appropriately trained IT security team available 24x7 to respond to viruses, unauthorized access and other security incidents? ☐ Yes ☐ No

45. Describe here, or on an attachment, any compensating security controls for questions answered "no" in Section IV:

V. AUDITS AND REVIEW

46. Are annual audits of physical, procedural and technical security controls performed by an independent security auditing organization with a CISSP or CISA certified practitioner on staff? ☐ Yes ☐ No

If "yes", name the vendor security organization(s):

47. Are vulnerability tests conducted at least annually on the following to make sure they perform as expected:

a.) External firewall?

☐ Yes ☐ No

b.) Intrusion detection / prevention systems?

☐ Yes ☐ No

c.) Website authentication services?

☐ Yes ☐ No

d.) Website software?

☐ Yes ☐ No

e.) Website servers and customer database servers?

☐ Yes ☐ No

48. Have all significant security risks identified by audit deficiencies, regulatory criticisms, vulnerability tests or exploited vulnerabilities been remediated? ☐ Yes ☐ No

If "no", indicate outstanding items and status of remediation on an attachment.

49. Is the individual in number 12 responsible for reporting the status of the program to executive management and / or the board of directors and if so, what is the frequency?

☐ No ☐ Longer than annually ☐ Annually ☐ Quarterly ☐ Monthly

50. At what frequency are information security and privacy policies reviewed and updated to reflect changes in business process, use of technology, new technology or software, security best-practices, and the regulatory environment?

☐ Monthly ☐ Quarterly ☐ Annually ☐ Longer than Annually

51. Does the information security program use a formal scoring or prioritization process for managing information security risks? ☐ Yes ☐ No

52. Within the last 12 months has the computer obtained an updated SAS70 Type II or other security audit for each vendor with access to electronic customer information? ☐ Yes ☐ No
☐ No vendors with access

53. Is the individual in number 12 responsible for monitoring the effectiveness of security procedures and controls? ☐ Yes ☐ No

54. Describe here, or on an attachment, any compensating security controls for questions answered "no" in Section V:

VI. INSURANCE COVERAGES AND UNDERWRITING INFORMATION

1. Do you currently have the prior or current insurance coverage listed below?

Coverage Type	Yes	No	Insurer	Limits	Deductible	Policy Period
Employment Liability						
Fiduciary Liability						
D&O Liability						
Trust Errors and Omissions Liability						
Internet and Electronic Banking Liability for FI						
Bankers Professional Liability						
Bankers Blanket Bond						

2. Coverage Requested

Coverage Type	Desired Limit	Desired Deductible
Internet and Electronic Banking Coverage		

3. Additional Underwriting Materials Requested

As part of this application, please attach the following:

- Attach proof of certification, if applicable (question number 24)
- Attach a description of previous security events (question numbers 22 and 38)
- Attach a description of outstanding risks and status of remediation efforts (question number 48)
- Attach a description of compensating controls (question numbers 15, 27, 38, 45 and 54)

4. Additional Underwriting Materials that may be Requested

As part of this application review process, CIC may request the following:

- Attach a representative sample of the information security provisions of third party vendor contracts (question number 30)
- Attach photocopy of website privacy policy and security statements (question number 17)
- Attach a photocopy of executive summary of the recent independent security audit for each vendor (question number 52)
- Attach a photocopy of security incident response procedures (question number 43)
- Attach a photocopy of the executive summary of the most recent independent IT security audit (question number 46)

Attached and made a part of this Renewal Proposal by reference is one copy of each of the following: the Company's most recent Annual Report and Statement of Condition to Stockholders, certified provisions of the Charter or Bylaws covering Indemnification of Directors and Officers, and Notice to Stockholders and Proxy Statement for either the last or the next annual meeting.

The Cincinnati Insurance Company is hereby authorized to make any investigation, inquiry and on-site security review in connection with this Renewal Proposal as it deems necessary.

The undersigned authorizes the release of claim information from any prior insurer to The Cincinnati Insurance Company.

Signing this Renewal Proposal does not bind the Company or The Cincinnati Insurance Company to complete the insurance.

PLEASE REVIEW CAREFULLY. Except to such extent as may be otherwise in the policy, the policy for which this Renewal Proposal is being made is limited for ONLY CLAIMS THAT ARE FIRST MADE AGAINST THE INSURED WHILE THE POLICY IS IN FORCE.

NOTICE TO FLORIDA APPLICANTS: ANY PERSON WHO KNOWINGLY AND WITH INTENT TO INJURE, DEFRAUD, OR DECEIVE ANY INSURER FILES A STATEMENT OF CLAIM OR AN APPLICATION CONTAINING ANY FALSE, INCOMPLETE, OR MISLEADING INFORMATION IS GUILTY OF A FELONY OF THE THIRD DEGREE.

NOTICE TO OHIO APPLICANTS: ANY PERSON WHO, WITH INTENT TO DEFRAUD OR KNOWING THAT HE / SHE IS FACILITATING A FRAUD AGAINST AN INSURER, SUBMITS AN APPLICATION OR FILES A CLAIM CONTAINING A FALSE OR DECEPTIVE STATEMENT IS GUILTY OF INSURANCE FRAUD.

WARNING: ANY PERSON WHO KNOWINGLY AND WITH INTENT TO DEFRAUD ANY INSURANCE COMPANY OR ANOTHER PERSON FILES AN APPLICATION FOR INSURANCE OR STATEMENT OF CLAIM CONTAINING ANY MATERIALLY FALSE INFORMATION, OR CONCEALS FOR THE PURPOSE OF MISLEADING INFORMATION CONCERNING ANY FACT MATERIAL THERETO, COMMITS A FRAUDULENT INSURANCE ACT, WHICH IS A CRIME AND SUBJECTS (VT: MAY BE COMMITTING A CRIME SUBJECTING) THE PERSON TO CRIMINAL AND (NY: SUBSTANTIAL) CIVIL PENALTIES. IN THE DISTRICT OF COLUMBIA, LOUISIANA, MAINE, TENNESSEE, VIRGINIA AND WASHINGTON, INSURANCE BENEFITS MAY ALSO BE DENIED.

Signed: _____
Chairman of the Board, President or comparable officer

Printed Name: _____

Title: _____

Date: _____

Signed: _____
Information Security Officer or comparable officer

Printed Name: _____

Title: _____

Date: _____

Agent's Signature

Date

Agency and Code Number

Agent's Name and License Number (Florida only)

SERFF Tracking Number: *CNNA-125314121*

State: *Arkansas*

Filing Company: *The Cincinnati Insurance Company*

State Tracking Number: *AR-PC-07-026341*

Company Tracking Number: *CBD-07-6023-AR*

TOI: *23.0 Fidelity*

Sub-TOI: *23.0000 Fidelity*

Product Name: *CBD-07-6023-AR*

Project Name/Number: */*

Rate Information

Rate data does NOT apply to filing.

SERFF Tracking Number: CNNA-125314121

State: Arkansas

Filing Company: The Cincinnati Insurance Company

State Tracking Number: AR-PC-07-026341

Company Tracking Number: CBD-07-6023-AR

TOI: 23.0 Fidelity

Sub-TOI: 23.0000 Fidelity

Product Name: CBD-07-6023-AR

Project Name/Number: /

Supporting Document Schedules

		Review Status:	
Bypassed -Name:	Uniform Transmittal Document-Property & Casualty	Approved	10/09/2007
Bypass Reason:	N/A		
Comments:			
		Review Status:	
Satisfied -Name:	PROPRETY AND CASUALTY TRANSMITTAL	Approved	10/09/2007
Comments:	PROPERTY AND CASUALTY TRANSMITTAL		
Attachment:	F777AR_307.pdf		
		Review Status:	
Satisfied -Name:	FORM FILING SCHEDULE	Approved	10/09/2007
Comments:	FORM FILING SCHEDULE		
Attachment:	F778AR_307.pdf		
		Review Status:	
Satisfied -Name:	MEMORANDUM	Approved	10/09/2007
Comments:	MEMORANDUM		
Attachment:	MEMOF.pdf		

Property & Casualty Transmittal Document

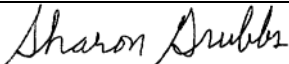
1. Reserved for Insurance Dept. Use Only	2. Insurance Department Use only	
	a. Date the filing is received:	
	b. Analyst:	
	c. Disposition:	
	d. Date of disposition of the filing:	
	e. Effective date of filing:	
	New Business	
	Renewal Business	
	f. State Filing #:	
	g. SERFF Filing #:	
h. Subject Codes		

3. Group Name	Group NAIC #
The Cincinnati Insurance Company	0244

4. Company Name(s)	Domicile	NAIC #	FEIN #	State #
The Cincinnati Insurance Company	Ohio	0244-10677	31-0542366	03

5. Company Tracking Number	CBD-07-6023-AR
-----------------------------------	-----------------------

Contact Info of Filer(s) or Corporate Officer(s) [include toll-free number]

6. Name and address	Title	Telephone #s	FAX #	e-mail
Sharon Grubbs 6200 South Gilmore Road Fairfield, Ohio 45014	Senior Filing Analyst	513-870-2091	513-870-2097	sharon_grubbs@cinfin.com
7. Signature of authorized filer				
8. Please print name of authorized filer		Sharon Grubbs		

Filing information (see General Instructions for descriptions of these fields)

9. Type of Insurance (TOI)	Bond
10. Sub-Type of Insurance (Sub-TOI)	Bond
11. State Specific Product code(s) (if applicable)[See State Specific Requirements]	n/a
12. Company Program Title (Marketing title)	n/a
13. Filing Type	<input type="checkbox"/> Rate/Loss Cost <input type="checkbox"/> Rules <input type="checkbox"/> Rates/Rules <input checked="" type="checkbox"/> Forms <input type="checkbox"/> Combination Rates/Rules/Forms <input type="checkbox"/> Withdrawal <input type="checkbox"/> Other (give description)
14. Effective Date(s) Requested	New: 05/01/08 Renewal:
15. Reference Filing?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
16. Reference Organization (if applicable)	n/a
17. Reference Organization # & Title	n/a
18. Company's Date of Filing	10/04/07
19. Status of filing in domicile	<input type="checkbox"/> Not Filed <input checked="" type="checkbox"/> Pending <input type="checkbox"/> Authorized <input type="checkbox"/> Disapproved

Property & Casualty Transmittal Document—

20.	This filing transmittal is part of Company Tracking #	CBD-07-6023-AR
------------	--	----------------

21.	Filing Description [This area can be used in lieu of a cover letter or filing memorandum and is free-form text]
------------	--

See Memorandum

22.	Filing Fees (Filer must provide check # and fee amount if applicable) [If a state requires you to show how you calculated your filing fees, place that calculation below]
<p>Check #: EFT FILING Amount: \$50</p> <p>Refer to each state's checklist for additional state specific requirements or instructions on calculating fees.</p>	

*****Refer to the each state's checklist for additional state specific requirements (i.e. # of additional copies required, other state specific forms, etc.)**

FORM FILING SCHEDULE

(This form must be provided ONLY when making a filing that includes forms)
 (Do not refer to the body of the filing for the forms listing, unless allowed by state.)

1.	This filing transmittal is part of Company Tracking #		CBD-07-6023-AR		
2.	This filing corresponds to rate/rule filing number (Company tracking number of rate/rule filing, if applicable)		N/A		
3.	Form Name /Description/Synopsis	Form # Include edition date	Replacement or Withdrawn?	If replacement, give form # it replaces	Previous state filing number, if required by state
01	PROPOSAL FOR CINCINNATI'S "BLUE CHIP" INSURANCE PROGRAM FOR FINANCIAL INSTITUTIONS - INTERNET AND ELECTRONIC BANKING PART VI	BC 010 11 07	<input type="checkbox"/> New <input checked="" type="checkbox"/> Replacement <input type="checkbox"/> Withdrawn	BC 010 11 07	CBD-07-6020-AR
02	RENEWAL PROPOSAL FOR CINCINNATI'S "BLUE CHIP" INSURANCE PROGRAM FOR FINANCIAL INSTITUTIONS - INTERNET AND ELECTRONIC BANKING COVERAGE PART VI	BC 011 11 07	<input type="checkbox"/> New <input checked="" type="checkbox"/> Replacement <input type="checkbox"/> Withdrawn	BC 011 10 07	CBD-07-6020-AR
03			<input type="checkbox"/> New <input type="checkbox"/> Replacement <input type="checkbox"/> Withdrawn		
04			<input type="checkbox"/> New <input type="checkbox"/> Replacement <input type="checkbox"/> Withdrawn		
05			<input type="checkbox"/> New <input type="checkbox"/> Replacement <input type="checkbox"/> Withdrawn		
06			<input type="checkbox"/> New <input type="checkbox"/> Replacement <input type="checkbox"/> Withdrawn		
07			<input type="checkbox"/> New <input type="checkbox"/> Replacement <input type="checkbox"/> Withdrawn		
08			<input type="checkbox"/> New <input type="checkbox"/> Replacement <input type="checkbox"/> Withdrawn		
09			<input type="checkbox"/> New <input type="checkbox"/> Replacement <input type="checkbox"/> Withdrawn		
10			<input type="checkbox"/> New <input type="checkbox"/> Replacement <input type="checkbox"/> Withdrawn		

**ARKANSAS
DIRECTORS AND OFFICERS LIABILITY
FORMS MEMORANDUM**

NEW FORM	OLD FORM	TITLE/DESCRIPTION OF CHANGE
		In this filing we are introducing the Internet and Electronic Banking Coverage Part (Part VI) for Financial Institutions.
BC 010 11 07	BC 010 10 07	PROPOSAL FOR CINCINNATI'S "BLUE CHIP" INSURANCE PROGRAM FOR FINANCIAL INSTITUTIONS - INTERNET AND ELECTRONIC BANKING COVERAGE PART VI Typographical errors corrected
BC 011 11 07	BC 011 10 07	RENEWAL PROPOSAL FOR CINCINNATI'S "BLUE CHIP" INSURANCE PROGRAM FOR FINANCIAL INSTITUTIONS - INTERNET AND ELECTRONIC BANKING COVERAGE PART VI Typographical errors corrected.